DOCUMENT P

Wayne B. Norris
2534 Murrell Road, Santa Barbara, CA 93109-1859
VOICE PHONE: 805-962-7703 FAX 801-365-4019
EMAIL wayne@WayneBNorris.com
URL http://WayneBNorris.com

9 July 2002

EXPERT WITNESS REPORT 4

Judge Dion G. Morrow, Retired
Court Appointed Discovery Referee
5101 Bedford Avenue
Los Angeles, CA 90056-1002

Re; Mitchell v Kasem, et al, BC 230326

To the Honorable Judge Morrow:

INTRODUCTION

I was asked by Plaintiff's Counsel, Mr. Bren C. Conner, to examine the first and last pages of a computer-generated 491-page report purported to be a list of the file contents of the hard disk drive of the Sun Microsystems SPARCstation computer that is the subject of this action.

I was further provided with significant dates in the evolution of the subject action.

The purpose of this examination in the background of the significant dates was to deduce possible or likely activity involving the subject computer relative to the significant dates, based on information in the report.

RESULTS OF INSPECTION

The report appeared to have been prepared by, or thru the use of, UNIX software created by Ontrack Data International, Inc., or one of its affiliated companies. Ontrack [http://www.ontrack.com] is a very well known and respected company in the field of disk data analysis and data recovery. The header on the report showed a date/time tag of 3/13/2002, 14:22:17.

The report showed a total of 412 million bytes of data on the hard drive, organized into 26,835 files, with no bad files, which is consistent with a fresh installation of the Solaris operating system onto a functioning disk. Solaris is the operating system created by Sun Microsystems for its product, the SPARCstation computer. Sun Microsystems is one of the world's largest computer hardware and software manufacturers. Solaris is an example of a group of operating systems known as the UNIX family, which are patterned after the original UNIX operating system designed by AT&T Bell Laboratories beginning in 1969.

A total of 51 files were listed on the two pages of the report I viewed. They were created on only FOUR different dates, as follows:

- 43 files were created on 5/25/2000, between 8:17 and 8:53. Significantly, among the 43 files were several that are typically created only during the initial installation of Solaris.
- 6 files were created on 4/20/2001, between 17:35 and 18::55
- 1 file was created on 8/24/200 at 18:04
- 1 file [an update file] was created on 7/16/1997 at 4:33

A further significant observation is that there were a total of 6 files in the `/var/tmp` directory whose names all followed the same formula: `wsconAAA??????_0.0`, where the question mark character is used to designate any character and the remaining characters are as shown.

Files of this type are well known to Solaris system administrators, but not widely known to casual users. They are undocumented by Sun, but are considered by experience and experimentation to be the result of a "bug" in Solaris. Files with this name-formula are typically created each time the system is booted in windowed mode. Their size tends to grow with the amount of activity carried on by the operator in windowed mode. They are always located in the same directory, and the name formula is always the same. The 6 characters designated by question marks are arbitrary, and are assigned by the system when each new file is created.

Of the total of 6 so-called "`wsconAAA`" files, the first – `wsconAAA0cPjuv_0.0` – was created on 5/25/2000 at 8:53, making it one of the last files created on that date. It contained 90 bytes of data. The next of these files was created on 8/24/2000 at 18:04. It contained zero bytes of data. The final 4 examples were all created on 4/20/2001, between 17:35 and 18:55. All contained zero bytes of data.

ANALYSIS and CONCLUSIONS

While there are thousands of files in the remaining portion of the report that I did not get to examine, the ones in the portion of the list that I did get to examine are highly consistent with one particular set of circumstances and highly inconsistent with any other set of reasonable circumstances.

SEQUENCE OF EVENTS

1. On Thursday, May 25, 2000, at just after 8:00 in the morning, by the system clock, someone reformatted the hard drive in question, and installed a fresh copy of the Solaris operating system. In general, this action would have destroyed all the data on the hard drive in existence up to that point. The facts that tend to support this are as follows:
    a. Even on the small list of files I was able to examine, there were several files that are generally only created and date-stamped during a fresh installation of Solaris. The opportunity to examine the first and last pages of the file list was significant, since the files were listed in alphabetical order

by both name and directory, and thus, the critical directories named "/", "`/.dt`", etc. were available for inspection.

b. The first files created, "`/bin`" and "`/lib`" – which are actually directory files – would logically be the first ones created during a fresh installation. Both were created at 8:17, by the system clock.

c. The apparent period of time from the first file time tag to the last – 36 minutes – is entirely consistent with a typical Solaris installation.

d. The trail left by the so-called "`wsconAAA`" files is also strongly consistent with the scenario described above. The first such file – `wsconAAA0cPjuv_0.0` – at 90 bytes long – was created on 5/25/2000 at 8:53, as one of the last files to be created on that day. This is entirely consistent with a typical Solaris installation, in which the windowed environment, called "CDE" for "Common Desktop Environment", is booted as one of the last tasks, creating the "`wsconAAA`" file as it does so, and capturing a small amount of activity into that file.

2. On August 24, 2000, at just after 6:00 PM, someone booted the computer. They must have gotten to the CDE windowed environment, because they created a "`wsconAAA`" file at 18:04, by the system clock, but they didn't do much, because that file is empty. Note that the creation of this type of file is one of the last stages of booting the system.

    a. This is the date the computer was received by Defendant's counsel, and they have admitted that they started the computer on that date.

3. On April 20, 2001, at just after 5:00 PM, someone booted the computer again. As previously, the must have gotten to the CDE windowed environment, because they created a "`wsconAAA`" file at 17:35, by the system clock. Also, as previously, they didn't do much, because that file is also empty.

4. On the same date, someone booted the computer a total of 3 more times. The final boot probably took place at about 18:52. One of the FIRST things created during a boot is a file called "`/.cpr_config`", a script created by and used by the `suspend/resume` utility. This file is overwritten on each session, so it does not leave a trail, like the "`wsconAAA`" files do. The existing copy of "`/.cpr_config`" was written at 18:52. Another file, "`/var/statmon/state`", has similar behavior, and that file was also written at 18:52. About 2 minutes must have elapsed until the CDE session started, since the "`wsconAAA`" file was written at 18:55 – about 5 minutes before 7:00 PM. None of these boot sessions did much, since their "`wsconAAA`" files were all empty.

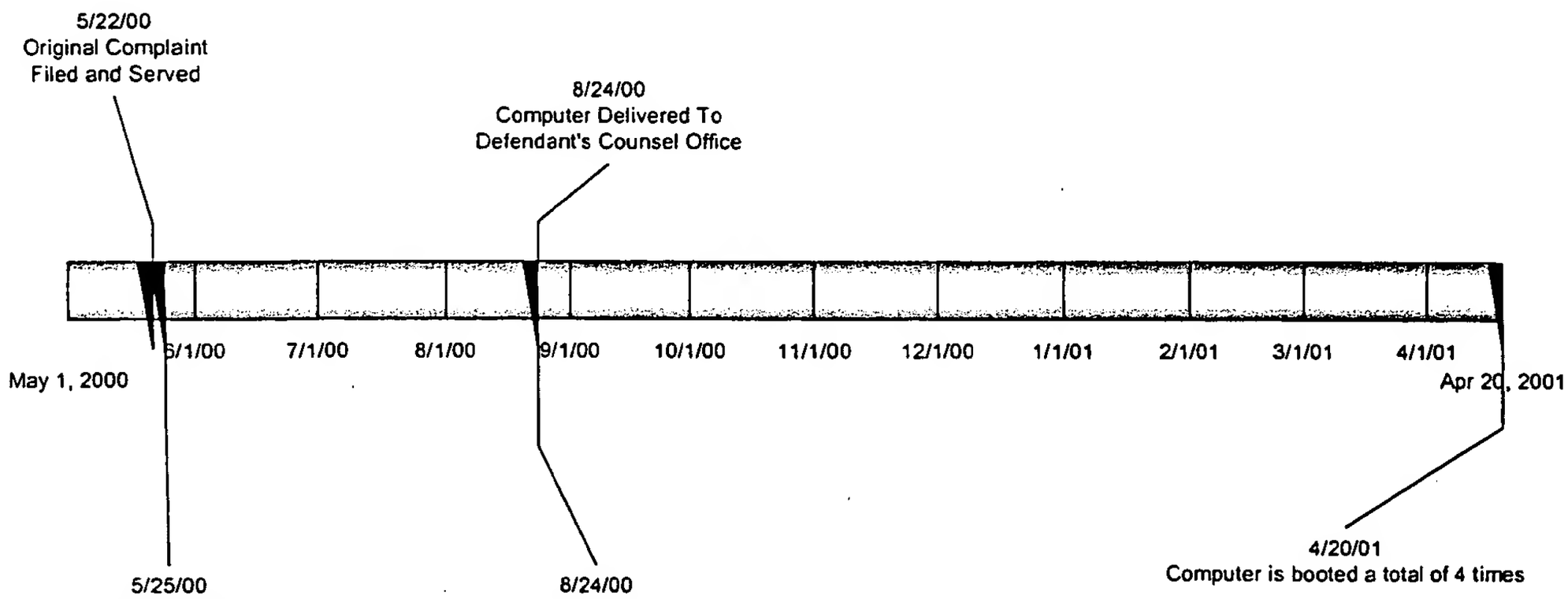
ANALYSIS

It is not possible to determine the contents of the hard drive prior to the time it was re-formatted on the morning of Thursday, May 25, 2000.

It is impossible to avoid noting the proximity [about 3 working days] of this event to the filing and service of the complaint in this case. Reformatting of a hard drive containing a Solaris operating system is not a trivial matter. Since such a process destroys all data on the disk, it is an extraordinary event, and normally would be preceded by a backup of the important data on the disk, followed by a restore of that data to the new operating system. There is no evidence to show that any data was restored, since at least on "`wsconAAA`" file following the reformatting should be non-empty if data were restored.

That leaves open the question of why the reformat was done in the first place. The apparent lack of user-generated data on a hard drive that was reformatted after prior use is unusual in the industry, to say the least. No legitimate purpose would seem to be served by destroying all the user-generated data on a disk and then not restoring it. A SPARCstation is a powerful professional tool, and destruction of data on one, without restoration, seems strange. Computer records, unfortunately, cannot directly answer questions of user motivation.

TIMELINE



RESPECTFULLY SUBMITTED,

WAYNE B. NORRIS